Method of controlling the operation of security modules

Patent Number: US4849927
Publication date: 1989-07-18
Inventor(s): VOS GERARDUS J F (NL)
Applicant(s):: NCR CO (US)
Requested Patent: DE3818960
Application Number: US19870099867 19870922
Priority Number(s): GB19870013734 19870612
IPC Classification: G06F9/00 ; G06F15/20 ; G06K5/00
EC Classification: G06F12/14B
Equivalents: CA1288492, FR2616561, GB2205667

Abstract

In a method of controlling the operation of a security module, wherein firmware controlling the operation of the security module (10) is stored in a program memory (40), new firmware may be loaded into the module (10). An authentication key (KA) is encrypted using a key storage key (KSK) stored in a resettable shift register (54) in the security module and the encrypted authentication key is stored in a secure memory (36). A firmware authentication value FAV is calculated, using the authentication key (KA), externally of the security module (10), for the new firmware, and the new firmware, together with FAV is loaded into a data memory (38) in the security module (10). A processor (30) in the security module (10) recalculates the firmware authentication value using the stored authentication key (KA) and compares the recalculated value with the loaded value FAV. If a correct comparison is achieved, the new firmware is transferred into the program memory (40). Otherwise, a reject status signal is issued and the firmware in the data memory (38) is erased.

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) Offenlegungsschrift

(11) DE 3818960 A1

(51) Int. Cl. 4: G 06 F 12/14

(21) Aktenzeichen: P 38 18 960.7
(22) Anmeldetag: 3. 6. 88
(43) Offenlegungstag: 22. 12. 88

DE 3818960 A1

(30) Unionspriorität: (32) (33) (31)
12.06.87 GB 13734/87

(71) Anmelder:
NCR Corp., Dayton, Ohio, US

(74) Vertreter:
Kahler, K., Dipl.-Ing., Pat.-Anw., 8948 Mindelheim

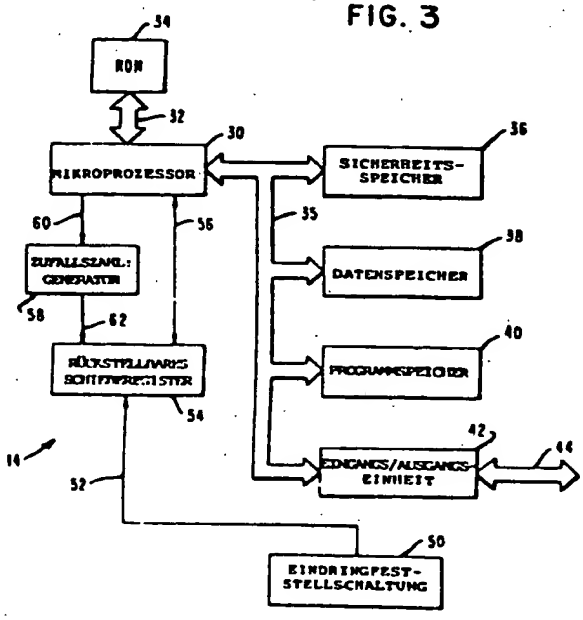
(72) Erfinder:
Vos, Gerardus Johannes Franciscus, Maarssen, NL

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Verfahren zum Steuern des Betriebes von Sicherheitsmodulen

Bei einem Verfahren zum Steuern des Betriebs eines Sicherheitsmoduls ist den Betrieb des Sicherheitsmoduls (10) steuernde Firmware in einem Programmspeicher (40) gespeichert. Neue Firmware kann in den Sicherheitsmodul (10) geladen werden. Ein Authentitätsschlüssel (KA) wird unter Verwendung eines Schlüsselspeicherschlüssels (KSK), der in einem rückstellbaren Schieberegister (54) in den Sicherheitsmodul gespeichert ist, verschlüsselt und der verschlüsselte Authentitätsschlüssel wird in einem Sicherheitsspeicher (36) gespeichert. Ein Firmwareauthentitätswert FAV wird unter Verwendung des Authentitätsschlüssels (KA) außerhalb des Sicherheitsmoduls (10) für die neue Firmware berechnet, und die neue Firmware wird zusammen mit dem FAV in einen Datenspeicher (38) in dem Sicherheitsmodul (10) geladen. Ein Prozessor (30) in dem Sicherheitsmodul (10) berechnet erneut den Firmwareauthentitätswert unter Verwendung des gespeicherten Authentitätsschlüssels (KA) und vergleicht den erneut berechneten Wert mit dem geladenen Wert FAV. Bei korrektem Vergleich wird die neue Firmware in dem Programmspeicher (40) geladen. Sonst wird ein Zurückweisungsstatussignal abgegeben und die Firmware in dem Datenspeicher (38) wird gelöscht.

FIG. 3



Patentansprüche

1. Ein Verfahren zum Steuern des Betriebs eines Sicherheitsmoduls mit Verarbeitungsvorrichtungen, einem Programmspeicher, der zum Speichern von Firmware für die Steuerung des Betriebs des Sicherheitsmoduls geeignet ist; Eingangs-/Ausgangsvorrichtungen und einem eindringresistenten Gehäuse, das die Abgabe eines Eindringanzeigesignals unter Ansprechen auf einen Versuch bewirkt, in das Gehäuse einzudringen, **gekennzeichnet durch** die Schritte: Eingeben eines Authentitätsschlüssels in den Sicherheitsmodul über die Eingangs-/Ausgangsvorrichtungen (42); Speichern des eingegebenen Authentitätsschlüssels Sichern in einer ersten Speichervorrichtung (36) in dem Sicherheitsmodul (10), wodurch der gespeicherte Authentitätsschlüssel unter Ansprechen auf die Abgabe des Eindringanzeigesignals nicht mehr greifbar wird: Berechnen eines ersten Firmwareauthentitätswertes außerhalb des Sicherheitsmoduls unter Verwendung der zu ladenden Firmware und des Authentitätsschlüssels, Eingeben der Firmware und des ersten Firmwareauthentitätswertes über die Eingangs-/Ausgangsvorrichtungen (42) in eine zweite Speichervorrichtung (38) in dem Sicherheitsmodul (10); Berechnen eines zweiten Firmwareauthentitätswertes in der Verarbeitungsvorrichtung (30) unter Verwendung der in der zweiten Speichervorrichtung (38) gespeicherten Firmware und des in der ersten Speichervorrichtung (36) gespeicherten Authentitätsschlüssels; Vergleichen des ersten und zweiten Authentitätswertes; übertragen der in der zweiten Speichervorrichtung (38) gespeicherten Firmware in den Programmspeicher (40) bei gültigem Vergleich; und Abgabe eines Zurückweisungsstatussignals im Falle eines ungültigen Vergleichs.

2. Ein Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Schritte Berechnen des ersten und zweiten Firmwareauthentitätswertes jeweils die aufeinanderfolgenden Schritte aufweisen: (a) Anordnen der Firmware in aufeinanderfolgenden Blocks, (b) Verschlüsseln des ersten Blocks der Firmware durch den Datenverschlüsselungsalgorithmus *DEA* unter Verwendung des Authentitätsschlüssels, (c) Anlegen des Ausgangswertes gemäß Schritt (b) zusammen mit einem zweiten Block der Firmware an eine EXCLUSIVE-ODER-Vorrichtung (106), (d) Verschlüsseln des EXCLUSIVE-ODER-Ausgangswertes des Schrittes (c) durch den Datenverschlüsselungsalgorithmus *DEA* unter Verwendung des Authentitätsschlüssels, (e) Wiederholen der Schritte (c) und (d) unter Verwendung der Ausgangswerte der entsprechenden vorhergehenden Schritte und aufeinanderfolgenden Blöcke der Firmware, bis alle Blöcke davon verwendet wurden, um einen letzten Ausgangsblock zu bilden, (f) Auswählen eines Teiles des letzten Ausgangsblocks als Firmwareauthentitätswert.

3. Ein Verfahren nach Anspruch 1 oder 2, gekennzeichnet durch den Schritt Erzeugen eines Schlüsselspeicherschlüssels und Laden des Schlüsselspeicherschlüssels in eine dritte Speichervorrichtung (54), wobei der Schritt Speichern des eingegebenen Authentitätsschlüssels die Schritte Verschlüsseln des Authentitätsschlüssels unter Verwendung des Schlüsselspeicherschlüssels als ein Verschlüsselungsschlüssel und Speichern des verschlüsselten Authentitätsschlüssels in der ersten Speichervorrichtung (36) beinhaltet.

4. Ein Verfahren nach Anspruch 3, dadurch gekennzeichnet, daß der Schritt Verschlüsseln des Authentitätsschlüssels den Schritt Anlegen des Authentitätsschlüssels und des Schlüsselspeicherschlüssels an eine EXCLUSIVE-ODER-Vorrichtung (90) beinhaltet.

5. Ein Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die dritte Speichervorrichtung einen rückstellbaren Schieberegisterspeicher (54) aufweist, der geeignet ist, unter Ansprechen auf die Abgabe des Eindringanzeigesignals zurückgestellt zu werden, wodurch der gespeicherte Authentitätsschlüssel nicht mehr zugreifbar gemacht wird.

6. Ein Verfahren nach einem der vorhergehenden Ansprüche, gekennzeichnet durch die Schritte Vorsehen von Speichervorrichtungen mit wahlfreiem Zugriff mit einem Programmspeicher (40) und der ersten und zweiten Speichervorrichtung (36, 38) und Speichern eines Firmwarezuordnungsblocks in den Speichervorrichtungen mit wahlfreiem Zugriff, um als Zeiger für die Anzeige der Position der Firmware zu dienen.

7. Ein Verfahren nach Anspruch 6, dadurch gekennzeichnet, daß der Schritt übertragen der in der zweiten Speichervorrichtung (38) gespeicherten Firmware in dem Programmspeicher (40) den Schritt Steuern des Firmwarezuordnungsblocks gemäß der Position der in der zweiten Speichervorrichtung gespeicherten Firmware beinhaltet.

8. Ein Verfahren nach einem der vorhergehenden Ansprüche, gekennzeichnet durch den Schritt Löschen der in der zweiten Speichervorrichtung (38) gespeicherten Firmware unter Ansprechen auf das Zurückweisungsstatussignal.

Beschreibung

Die Erfindung betrifft ein Verfahren zum Steuern des Betriebs von Sicherheitsmodulen.

Grundsätzlich weist ein Sicherheitsmodul, das auch als einbruchresistentes Modul bezeichnet wird, ein stabiles und sicheres Gehäuse auf, das Verarbeitungsvorrichtungen und Speichervorrichtungen zum Speichern sensitiver Daten enthält. Ein Versuch, in den Sicherheitsmodul einzudringen, beispielsweise das Gehäuse aufzubrechen oder zu durchbohren, führt zu einer Rückstellung der Speichervorrichtung, die die sensitiven Daten speichert.

Sicherheitsmodule finden Anwendung in Datenverarbeitungssystemen und -netzwerken, wo ein hoher Sicherheitsgrad wesentlich ist. Derartige Anwendungen sind beispielsweise elektronische Zahlungssysteme, elektronische Geldüberweisungssysteme (EFT), Datenentschlüsselung und -verschlüsselung; Prüfung einer persönlichen Identifikationsnummer (PIN), Zugangskontrolle und Abwicklung von Bankvorgängen von zu Hause.

Die U.S. P.S. 45 93 384 offenbart ein Sicherheitsmodul mit einem keramischen Gehäuse, das aus sechs miteinander verbundenen Teilen gebildet wird und einen Prozessor und ein rückstellbares Schieberegister zum Speichern sensitiver Daten enthält. Jeder Teil des Gehäuses ist mit einem Paar von Leitungswegabschnitten versehen, die in übereinandergelagerten Schichten angeord-

net sind und eine komplementäre Zickzackkonfiguration aufweisen. Die Leitungswegabschnitte auf den Gehäuseteilen sind miteinander verbunden und bilden einen ersten und zweiten Leitungsweg. Eine Unterbrechung eines der Leitungswege oder ein Kurzschluß zwischen ihnen aufgrund eines Versuchs, in das Gehäuse einzudringen, bewirkt, daß ein Rückstellsignalgenerator ein Rückstellsignal zum Löschen des Inhalts des rückstellbaren Schieberegisters gibt. Eine Temperatursensorschaltung, die darauf anspricht, daß die Temperatur in dem Gehäuse unter einen vorbestimmten Wert fällt, bewirkt ebenfalls die Abgabe eines Rückstellsignals durch den Rückstellsignalgenerator, um das rückstellbare Schieberegister zurückzustellen. Der bekannte Sicherheitsmodul enthält einen programmierbaren Nur-Lesen-Speicher (PROM), der das EDV-Programm für den Sicherheitsmodul, d. h. das vom Prozessor auszuführende Softwareprogramm speichert.

Der bekannte Sicherheitsmodul hat den Nachteil einer geringen betriebsmäßigen Flexibilität. Da die Funktionsfähigkeit des bekannten Sicherheitsmoduls bestimmt wird durch die in dem PROM-Speicher gespeicherte Firmware und da PROM-Speicher durchwegs mittels spezieller PROM-Programmiervorrichtungen in einer nicht mehr umkehrbaren Weise programmiert werden, ist es nach der Montage und dem Verschließen des den PROM-Speicher umgebenden bekannten Sicherheitsmodul nicht mehr möglich, Änderungen in der Funktion des bekannten Sicherheitsmoduls vorzunehmen. Derartige Änderungen sind jedoch wünschenswert, wenn das System, in dem der Sicherheitsmodul verwendet wird, erweitert oder verbessert werden soll.

Der Erfindung liegt die Aufgabe zugrunde, ein Verfahren zum Steuern des Betriebs eines Sicherheitsmodul anzugeben, bei dem derartige Module einen hohen Grad an Betriebsflexibilität aufweisen.

Diese Aufgabe wird gelöst durch ein Verfahren zum Steuern des Betriebs eines Sicherheitsmoduls mit Verarbeitungsvorrichtungen, einem Programmspeicher, der zum Speichern von Firmware für die Steuerung des Betriebs des Sicherheitsmoduls geeignet ist; Eingangs-/Ausgangsvorrichtungen und einem eindringresistenten Gehäuse, das die Abgabe eines Eindringanzeigesignals unter Ansprechen auf einen Versuch bewirkt, in das Gehäuse einzudringen, gekennzeichnet durch die Schritte: Eingeben eines Authentitätsschlüssels in den Sicherheitsmodul über die Eingangs-/Ausgangsvorrichtung; Speichern des eingegebenen Authentitätsschlüssels Sichern in einer ersten Speichervorrichtung in dem Sicherheitsmodul, wodurch der gespeicherte Authentitätsschlüssel unter Ansprechen auf die Abgabe des Eindringanzeigesignals nicht mehr greifbar wird; Berechnen eines ersten Firmwareauthentitätswertes außerhalb des Sicherheitsmoduls unter Verwendung der zu ladenden Firmware und des Authentitätsschlüssels, Eingeben der Firmware und des ersten Firmwareauthentitätswertes über die Eingangs-/Ausgangsvorrichtungen in eine zweite Speichervorrichtung in dem Sicherheitsmodul; Berechnen eines zweiten Firmwareauthentitätswertes in der Verarbeitungsvorrichtung unter Verwendung der in der zweiten Speichervorrichtung gespeicherten Firmware und des in der ersten Speichervorrichtung gespeicherten Authentitätsschlüssels; Vergleichen des ersten und zweiten Authentitätswertes; Übertragen der in der zweiten Speichervorrichtung gespeicherten Firmware in dem Programmspeicher bei gültigem Vergleich; und Abgabe eines Zurückweisungsstatussignals im Falle eines ungültigen Vergleichs.

Es zeigt sich somit, daß mit dem erfindungsgemäßen Verfahren die Funktion eines Sicherheitsmoduls in zuverlässiger Weise in einer nicht gesicherten Umgebung geändert werden kann. Soll somit ein derartiges System, das einen erfindungsgemäßen Sicherheitsmodul verwendet, erweitert oder verbessert werden, dann kann die den Betrieb des Sicherheitsmodul steuernde Firmware in zuverlässiger Weise in einer nicht gesicherten Umgebung an einem Ort geändert werden, an dem der Sicherheitsmodul installiert und in Gebrauch ist.

Ein weiterer Vorteil des erfindungsgemäßen Verfahrens besteht darin, daß ein standardisierter Sicherheitsmodul hergestellt und an einen Kunden geliefert werden kann, wo die gewünschte Firmware in einer nicht gesicherten Umgebung in den Sicherheitsmodul geladen wird. Es ergibt sich somit ein verhältnismäßig kostengünstiges Herstellungsverfahren.

Es ist weiterhin ersichtlich, daß die Vorteile der Erfindung erreicht werden, ohne daß kostspielige Speichervorrichtungen, wie EPROM-Speicher (löschbare, programmierbare Nur-Lesen-Speicher) oder EAROM-Speicher (elektrisch änderbare Nur-Lesen-Speicher) verwendet werden. Bei EPROM-Speichern ist es durchwegs erforderlich, die gespeicherte Information zu löschen, bevor neue Informationen eingegeben werden können, wobei ein derartiges Löschen durchwegs mittels UV-Licht durchgeführt wird. Dies bedeutet aber, daß ein EPROM-Speicher nicht mehr umprogrammiert werden kann, sobald die Vorrichtung einmal in dem geschlossenen Sicherheitsmodul eingebracht worden ist. EAROM-Speicher sind zwar bekannt; sie sind jedoch teuer und erfordern spezielle hohe Spannungen für die Umprogrammierung, die innerhalb eines geschlossenen Sicherheitsmoduls nur schwierig zu erzeugen und/oder zu kontrollieren sind.

Bevorzugte Weiterbildungen des erfindungsgemäßen Verfahrens sind in den Unter-Ansprüchen gekennzeichnet.

Weitere Merkmale und Vorteile des erfindungsgemäßen Verfahrens ergeben sich aus der nachfolgenden Beschreibung eines Ausführungsbeispiels anhand der Zeichnung. Es zeigen

Fig. 1 eine Perspektivansicht eines Sicherheitsmoduls

Fig. 2 eine auseinandergezogene Perspektivansicht verschiedener Teile des Gehäuses des Sicherheitsmoduls nach Fig. 1

Fig. 3 ein schematisches Blockschaltbild der Schaltung innerhalb des Sicherheitsmoduls gemäß Fig. 1

Fig. 4 ein schematisches Blockschaltbild einer Eindringfeststellschaltung in der Schaltung gemäß Fig. 3

Fig. 5 ein Funktionsdiagramm zur Veranschaulichung, wie ein Authentitätsschlüssel gespeichert und ausgelesen wird

Fig. 6 ein Diagramm zur Veranschaulichung des Formats der in den Sicherheitsmodul zu ladenden Firmware

Fig. 7 ein Diagramm zur Veranschaulichung eines Algorithmus, der zur Erzeugung eines Firmware-Authentitätswertes verwendet wird

Fig. 8 eine Einrichtung, die zum Laden der Firmware in den Sicherheitsmodul verwendet wird und

Fig. 9 ein Flußdiagramm zur Veranschaulichung des beim Laden der Firmware in den Sicherheitsmodul verwendeten Ablaufs.

Es wird zunächst auf die Fig. 1 und 2 Bezug genommen, die einen Sicherheitsmodul (10) zeigen, der ein eine elektronische Schaltung (14) (Fig. 2) enthaltendes Gehäuse (12) zeigt. Das Gehäuse besteht aus einer Deckplatte *P1*, Seitenplatten *P2*—*P5* und einer Bodenplatte

P6. Die sechs Platten P1 – P6 sind vorzugsweise aus keramischem Material hergestellt, da keramisches Material hochresistent gegen chemische Einflüsse ist. Die auf der Bodenplatte P6 angebrachte elektronische Schaltung (14) ist mittels in Fig. 2 nicht gezeigter Leitungen (16) mit Anschlußbereichen (18) verbunden, die an einem Randabschnitt (20) der Bodenplatte P6 angebracht sind. Die Anschlußbereiche (18) sind in Kontakt mit entsprechenden, nicht gezeigten Eingangs-/Ausgangsstiften, wodurch in üblicher Weise Verbindungen zu externen Schaltungen hergestellt werden, wobei der Sicherheitsmodul (10) auf einer nicht gezeigten, gedruckten Schaltungsplatte angebracht ist. Alternativ dazu kann auch eine Stecker-/Buchsenverbindung vorgesehen sein.

Jede der sechs Platten trägt ein Paar nicht gezeigter Leitungswegsegmente, wobei die Leitungswegsegmente auf den entsprechenden Platten P1 – P6 miteinander verbunden sind, so daß sie zwei Drahtgitter bilden. Die Drahtgitter sind mit einer Eindringfeststellschaltung zum Schützen des Sicherheitsmodul (10) gegen unautorisiertes Eindringen verbunden, wie dies später noch beschrieben wird. Die genaue Konfiguration der Drahtgitter ist für die vorliegende Erfindung nicht wesentlich. Beispiele möglicher Konfigurationen sind in der vorbenannten US-PS 45 93 384 und in der veröffentlichten britischen Patentanmeldung 21 82 176 beschrieben. Wenn ein niedrigerer Sicherheitsgrad ausreicht, kann auch eine Konfiguration bestehend aus nur einem Gitter genügen.

Es wird nun auf Fig. 3 Bezug genommen, die ein Blockschaltbild der Schaltung (14) zeigt, die innerhalb des Gehäuses (12) des Sicherheitsmodul (10) untergebracht ist. Die Schaltung (14) umfaßt einen Mikroprozessor (30), der über eine Sammelleitung (32) mit einem ROM-Speicher (34) verbunden ist. Der Mikroprozessor (30) steht auch über eine Sammelleitung (35) mit einem Sicherheitsspeicher (36), einem Datenspeicher (38), einem Programmspeicher (40) und einer Eingangs-/Ausgangseinheit (I/O-Einheit) (42) in Verbindung, die über eine Sammelleitung (44) mit den Anschlußbereichen (18) (Fig. 3) des Sicherheitsmoduls (10) verbunden ist.

Der Sicherheitsspeicher (36), der Datenspeicher (38) und der Programmspeicher (40) sind als RAM-Speicher (Speicher mit wahlfreiem Zugriff) ausgebildet und können gebildet werden durch einen oder mehrere im Handel erhältliche RAM-Vorrichtungen, etwa derart, daß der Sicherheitsspeicher (36), der Datenspeicher (38) und der Programmspeicher (40) entsprechende Abschnitte eines einzigen Adressenbereichs bilden. Der Sicherheitsspeicher (36) speichert Informationen, die unzugänglich gemacht werden, wenn bei einem Versuch, Zugriff zu der darin gespeicherten Information zu erhalten, in den Sicherheitsmodul (10) eingedrungen wird. Der Datenspeicher (38) und der Programmspeicher (40) speichern Daten- bzw. Programm-Informationen.

Die Schaltung (14) enthält eine Eindringfeststellschaltung (50), die über eine Leitung (52) mit einem rückstellbaren Schieberegister (54) verbunden ist. Das Schieberegister (54) ist an den Mikroprozessor (30) über eine Leitung (56) angeschlossen. Ein Zufallszahlengenerator (58) steht mit dem Mikroprozessor (30) über eine Leitung (60) und über eine Leitung (62) mit dem Schieberegister (54) in Verbindung.

Es wird nun auf Fig. 4 Bezug genommen, welche zeigt, daß die Eindringfeststellschaltung (50) zwei Drahtgitter (70 und 72), an sich meanderförmig gelegte Schleifen aufweist, die auf den das Gehäuse (12) in zuvor erläuterter Weise bildenden Platten P1 – P6 angeordnet sind. Das Drahtgitter oder -netz (70) ist mit einem Anschluß (74) verbunden, der an Erde liegt, und an einem Anschluß (76), der mit einer Fühlschaltung HL (78) verbunden ist. Das Drahtgitter (72) ist mit einem Anschluß (80) verbunden, an dem eine Versorgungsspannung V liegt, sowie mit einem Anschluß (82), der mit einer Fühlschaltung (84) in Verbindung steht. Die Fühlschaltungen (78 und 84) sowie ein Niedertemperatursensor (86) sind gemeinsam an einen Niederspannungsdetektor (88) verbunden, dessen Ausgang an die Leitung (52) (Fig. 3) angeschlossen ist. Kurz gesagt, führt ein Versuch, in das Gehäuse (12) des Sicherheitsmoduls (10) mittels Durchbohren oder Aufbrechen des Gehäuses (12) zu einer Unterbrechung eines oder beider Drahtgitter (70, 72) oder zu einem Kurzschluß zwischen diesen. Diese Zustände werden mittels der Fühlschaltungen (78, 84) festgestellt und es wird ein niedriges Ausgangsspannungssignal erzeugt, das in dem Niederspannungsdetektor (88) ein RESET-Ausgangssignal auf Leitung (52) bewirkt. Ein Versuch, den Sicherheitsmodul (10) unter eine vorbestimmte Temperatur abzukühlen und dadurch den Inhalt des rückstellbaren Schieberegisters (54) "einzufrieren", erzeugt im Niedertemperatursensor (86) ein niedriges Spannungssignal, das wiederum den Niederspannungsdetektor (88) veranlaßt, das RESET-Signal auf Leitung (52) abzugeben. Das RESET-Signal dient dazu, das rückstellbare Schieberegister (54) (Fig. 3) zurückzustellen.

Es sei nun wieder auf Fig. 3 Bezug genommen. Der Programmspeicher (40) speichert in einem RAM-Speicher die Firmware (Steuerprogramm), das die Funktion des Sicherheitsmoduls (10) steuert und bestimmt.

Nachdem der Sicherheitsmodul (10) zusammengesetzt, geprüft und verschlossen wurde, erfolgt eine Initialisierungsoperation unter Steuerung einer Initialisierungsroutine, die in dem ROM-Speicher (34) (Fig. 3) gespeichert ist. Gemäß Fig. 5 bewirkt die Initialisierungsoperation die Abgabe eines Signals durch den Mikroprozessor auf Leitung (60), um den Zufallszahlengenerator (58) für die Erzeugung einer 64-bit-Zufallszahl anzustoßen, die in dem rückstellbaren Schieberegister (54) gespeichert und nachstehend als Schlüsselspeicherschlüssel *KSK* bezeichnet wird. Als nächstes wird bei der Initialisierungsoperation ein 64-bit-Authentitätsschlüssel *KA* an den Sicherheitsmodul (10) über die Sammelleitung (44) und die Eingangs-/Ausgangseinheit (42) angelegt. Der Authentitätsschlüssel *KA* wird dann unter Verwendung des *KSK* dadurch verschlüsselt, daß der *KA* und der *KSK* an eine EXCLUSIVE-ODER-Schaltung (90) im Mikroprozessor (30) angelegt wird. Alternativ dazu kann die EXCLUSIVE-ODER-Funktion auch in dem Mikroprozessor (30) mittels einer Software-Routine im ROM-Speicher (34) durchgeführt werden. Ferner besteht die Möglichkeit, an Stelle der EXCLUSIVE-ODER-Verschlüsselung beispielsweise eine volle DES-Verschlüsselung (gemäß dem Datenverschlüsselungstandard) durchzuführen, die 16 Zyklen der DES-Verschlüsselungsoperation umfaßt, oder eine geringere Anzahl derartiger Zyklen, beispielsweise vier Zyklen, können angewandt werden. Der verschlüsselte Authentitätsschlüssel *KA* wird dann in dem Sicherheitsspeicher (36) gespeichert.

Nach dem Laden des Authentitätsschlüssels *KA* in verschlüsselter Form in den Sicherheitsspeicher (36) setzt sich die Initialisierungsoperation durch Laden einer ersten Firmware für den Sicherheitsmodul über die Eingangs-/Ausgangseinheit (42) in dem Programmspei-

cher (40) fort. In dem Programmspeicher (40) wird auch eine zusätzliche Laderoutine eingebracht, die dann verwendet wird, wenn es gewünscht wird, in den Programmspeicher eine neue Firmware zu laden.

Es ist verständlich, daß die zuvor beschriebene Initialisierungsoperation in Sicherheitsumgebung durchgeführt wird, wo die Sicherheit des Authentitätsschlüssels *KA* und der anfänglichen Firmware garantiert werden kann. Nun wird der Sicherheitsmodul in ein Datenterminal oder -endgerät eingebaut, beispielsweise einer EFT-POS-Einrichtung, also einem Waren-Abrechnungssystem mit automatischer elektronischer Überweisung, wobei dieser Einbau an Ort und Stelle erfolgen kann. Soll dann die Firmware erweitert oder geändert werden, um die Funktion des Sicherheitsmoduls (10) aufzustufen oder zu verändern, dann wäre es teuer und zeitaufwendig, wenn der Sicherheitsmodul von seinem Einsatzort in einen Sicherheitsbereich eingesandt werden müßte.

Die vorliegende Erfindung bringt die Möglichkeit, neue Firmware in den Sicherheitsmodul in zuverlässiger Weise am Einsatzort zu laden.

Es sei nun angenommen, daß eine neue Firmware *F* in den Sicherheitsmodul (10) zu laden ist. Fig. 6 veranschaulicht schematisch die in den Sicherheitsmodul (10) zu ladende neue Firmware *F*, bestehend aus n bytes. Die neue Firmware *F* ist in m Blöcke mit jeweils 64 bits unterteilt, wobei Nullen dazu verwendet werden können, den Endblock zu kennzeichnen. Die neue Firmware kann somit dargestellt werden als $F = F_1 F_2 \ldots F_m$, wobei $F_1, F_2, \ldots, F_m$ aus jeweils 64 bits besteht. Ein Firmwareauthentitätswert *FAV*, bestehend aus 4 bytes, wird dann gemäß dem Algorithmus in Fig. 7 berechnet.

Gemäß Fig. 7 wird der Algorithmus in *m* Zeitperioden $T_1, T_2, \ldots, T_m$ durchgeführt. Während der Zeitperiode T_1 wird der 64-bit-Block F_1 als Eingangswert I_1 (Block 100) an den DEA-Block (102) (Datenverschlüsselungsalgorithmus) angelegt, wobei *KA* als DEA-Schlüssel verwendet wird. Es sei darauf hingewiesen, daß der Datenverschlüsselungsalgorithmus (DEA) ein Standardalgorithmus ist, der in Fachveröffentlichungen, wie der Veröffentlichung FIPS (Federal Information Processing Standards), Publication No. 46, beschrieben ist. Der Ausgangswert 01 (Block 104) der DEA-Berechnung wird an eine EXCLUSIVE-ODER-Vorrichtung (105) zusammen mit dem nächsten 64-bit-Firmwareblock F_2 angelegt (Block 108). Während der Zeitperiode T_2 wird der Ausgangswert der EXCLUSIVE-ODER-Vorrichtung (105) als Eingangswert I_2 (Block 110) einer zweiten DEA-Berechnung unterzogen (Block 112), wobei wiederum der Authentitätsschlüssel *KA* verwendet wird. Der Vorgang wird in gleicher Weise fortgesetzt, bis der letzte 64-bit-Firmwareblock F_m verwendet wurde (Block 114) und sich ein letzter Ausgangswert O_m ergibt (Block 116). Die am weitesten links befindlichen 32 Bits des letzten Ausgangswertes O_m werden dann als Firmwareauthentitätswert *FAV* genommen. Dieser *FAV* wird dann an die Firmware *F* als weitere 4 bytes $n + 1, \ldots, n + 4$ angehängt (Fig. 6). Es sei darauf hingewiesen, daß der im Zusammenhang mit Fig. 7 beschriebene Algorithmus lediglich ein Beispiel darstellt und daß andere Algorithmen dazu verwendet werden können, den Firmwareauthentitätswert *FAV* zu bestimmen.

Es sei ferner darauf hingewiesen, daß der Firmwareauthentitätswert *FAV* auch unter Verwendung eines geeignet programmierten Prozessors oder bei dafür spezialisierter Hardware erzeugt werden kann.

Fig. 8 zeigt schematisch eine Einrichtung zum Laden der neuen Firmware in den Sicherheitsmodul (10). Die Einrichtung verwendet einen Personalcomputer (120) mit einer Verbinderplatte (122), die mittels eines Kabels (124) mit einer Verbinderbox (126) verbunden ist. Der Sicherheitsmodul (10) wird in die Verbinderbox (126) eingesteckt. Eine die neue Firmware *F* und den zugehörigen Firmwareauthentitätswert *FAV* enthaltende, nicht gezeigte Diskette wird dann in eine Diskettenstation (128) in dem Personalcomputer (120) eingesetzt. Unter Programmsteuerung bewirkt nun der Personalcomputer (120), daß die neue Firmware und der zugeordnete *FAV* über die Verbinderplatte (122), das Kabel (124) und die Verbinderbox (126) an den Sicherheitsmodul angelegt wird.

Fig. 9 zeigt ein Flußdiagramm für den Ladevorgang für die neue Firmware. Das Flußdiagramm beginnt mit dem Block 130. Die neue Firmware zusammen mit dem zugeordneten *FAV* wird an den Sicherheitsmodul (10) angelegt, wie dies im Zusammenhang mit Fig. 8 beschrieben wurde, und über die Eingangs-/Ausgangseinheit (42) (Fig. 3) dem Datenspeicher (Fig. 3) zugeführt. Als nächstes bewirkt die in dem Programmspeicher (40) (Fig. 3) gespeicherte zusätzliche Laderoutine (vgl. auch Fig. 5), daß der Schlüsselspeicherschlüssel *KSK* aus dem rückstellbaren Schieberegister (54) zusammen mit dem verschlüsselten Authentitätsschlüssel *KAENCR* an eine EXCLUSIVE-ODER-Vorrichtung (92) angelegt wird, die sich im Mikroprozessor (30) befindet. Der Ausgangswert der EXCLUSIVE-ODER-Vorrichtung (92) ist ein Klartextwert des Authentitätsschlüssels *KA*. Falls die EXCLUSIVE-ODER-Vorrichtung (90) durch eine kompliziertere Verschlüsselungsvorrichtung oder ein Verschlüsselungsprogramm ersetzt wird, dann wird die EXCLUSIVE-ODER-Vorrichtung (92) ersetzt durch eine entsprechende Verschlüsselungsvorrichtung oder Verschlüsselungsroutine.

Es sei nun wieder auf Fig. 9 Bezug genommen, die zeigt, daß die zusätzliche Laderoutine als nächstes bewirkt, daß die neue Firmware an den Mikroprozessor (30) angelegt wird, wo der in Fig. 7 gezeigte Algorithmus unter Verwendung des Schlüssels *KA* angewandt wird, um einen Firmwareauthentitätswert *FAV'* zu berechnen. Der Algorithmus kann in dem ROM-Speicher (34) oder in dem Programmspeicher (40) gespeichert sein. Im Block 136 wird ein Vergleich dahingehend durchgeführt, ob *FAV'* = *FAV*. Ist der Vergleich positiv, dann wird die Firmware von dem Datenspeicher (38) in den Programmspeicher (40) (Block 138) übertragen, ein Annahmestatussignal wird abgegeben und die zusätzliche Laderoutine endet mit Block 140. Ist der Vergleich negativ, dann wird gemäß Block 142 die Firmware zurückgewiesen und die Vergleichsoperation bewirkt ein Zurückweisungssignal, das zur Folge hat, daß die in dem Datenspeicher (38) gespeicherte Firmware gelöscht wird und die zusätzliche Laderoutine mit Block 144 endet.

Es sei bemerkt, daß im Falle eines positiven Vergleichs zwischen *FAV'* und *FAV* die neue Firmware von dem Datenspeicher (38) in den Programmspeicher (40) übertragen wird. Es sei darauf hingewiesen, daß eine derartige Übertragung nicht physisch erfolgen muß. So speichert der den Sicherheitsspeicher (36), den Datenspeicher (38) und den Programmspeicher (40) bildende RAM-Speicher einen Firmwarezuordnungsblock (*FAB*), der als Zeiger dazu dient, die Position der Firmware anzugeben. Bei einer geeigneten Änderung im Firmwarezuordnungsblock *FAB* erfolgt die Übertragung der neuen Firmware von dem Datenspeicher (38)

zum Programmspeicher (40) ohne eine physische Bewegung der Firmware zwischen den RAM-Speicherpositionen.

Somit wurde der Sicherheitmodul (10) in zuverlässiger Weise mit neuer Firmware geladen. Es sei bemerkt, daß bei einem Versuch, in den Sicherheitsmodul (10) eine Firmware zu laden, die in unerlaubter Weise modifiziert wurde, der Vergleich zwischen *FAV'* und *FAV* negativ wäre, was zu einer Zurückweisung der Firmware führt. Es sei ferner darauf hingewiesen, daß die Funktion des Sicherheitsmoduls (10) durch Laden der neuen Firmware ohne weitere Sicherheitsvorkehrungen am Einsatzort erfolgen kann, ohne daß er Sicherheitsmodul in einem Sicherheitsbereich eingeschickt werden müßte.

Es wird darauf hingewiesen, daß jeglicher Versuch, in den Sicherheitsmodul einzudringen oder diesen aufzubrechen, die Abgabe des RESET-Signals auf Leitung (52) zur Folge hat. Ein derartiges RESET-Signal bewirkt die Rückstellung des rückstellbaren Schieberegisters (54) und damit die Löschung des Schlüsselspeicherschlüssels *KSK*. Ist dieser *KSK* gelöscht, dann ist der Authentitätsschlüssel *KA*, der in dem Sicherheitsspeicher (36) als *KAENCR* gespeichert ist, nicht mehr greifbar, da er nicht mehr entschlüsselt werden kann, und somit läßt sich auch der Sicherheitsmodul (10) nicht mehr mit neuer Firmware laden. Somit wird ein möglicher Mißbrauch des Sicherheitssystems, das den Sicherheitsmodul (10) verwendet, aufgrund einer nicht erlaubten Entdeckung des Authentitätsschlüssels *KA* verhindert.

Nummer: 38 18 960
Int. Cl.⁴: G 06 F 12/14
Anmeldetag: 3. Juni 1988
Offenlegungstag: 22. Dezember 1988

3818960

FIG. 1

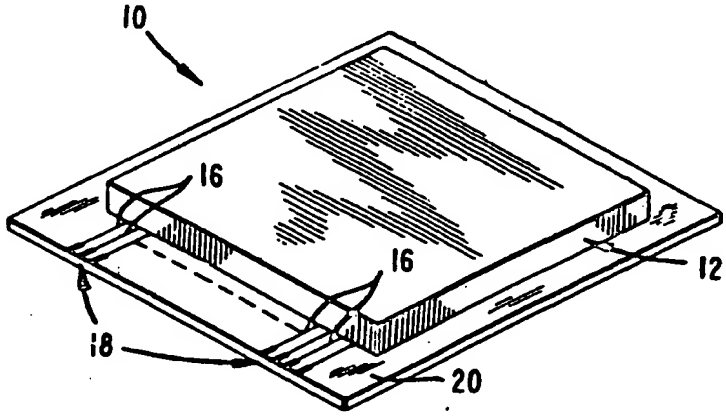
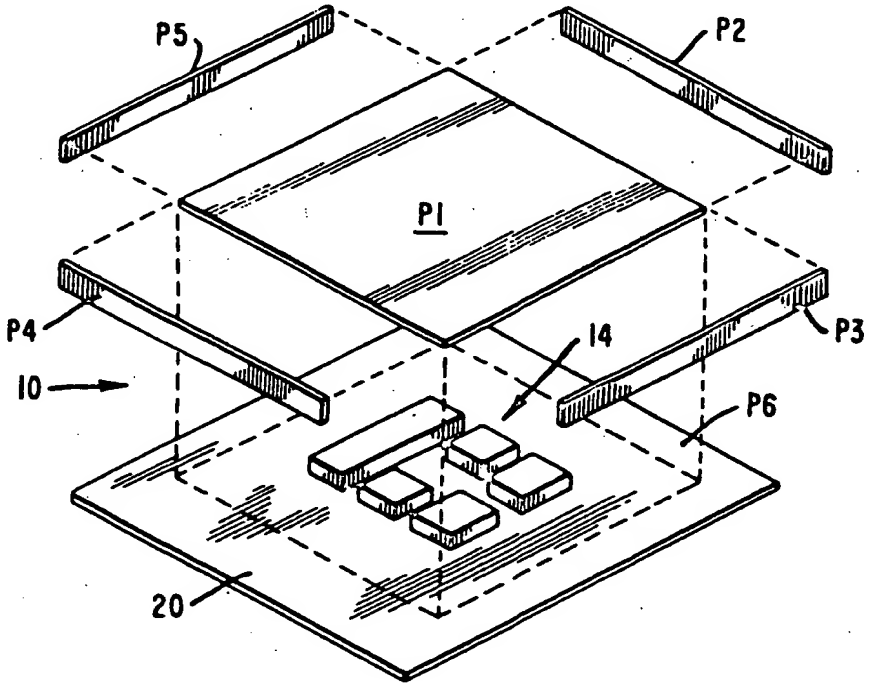
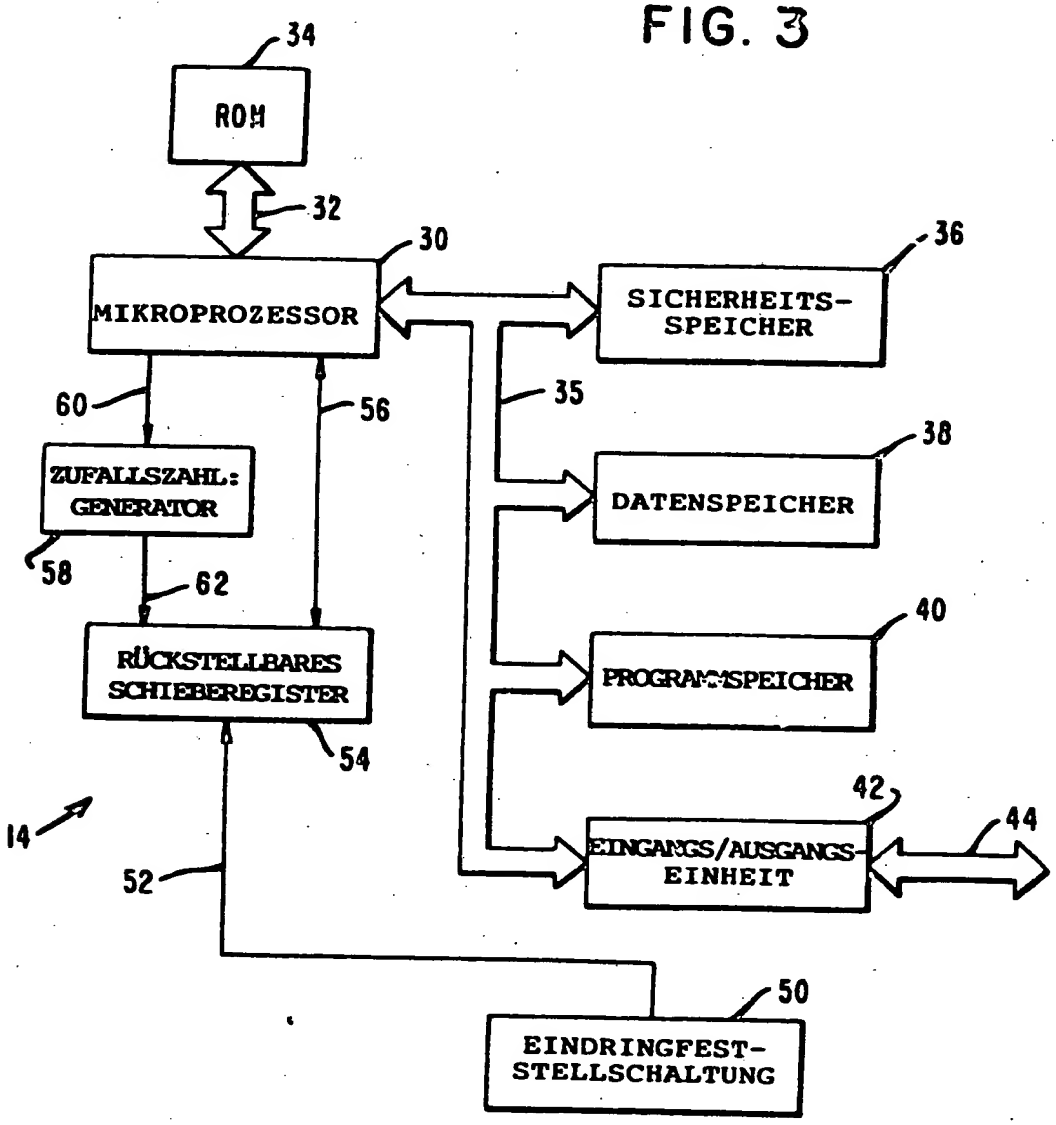


FIG. 2



3818960

FIG. 3



22

3818960

FIG. 4

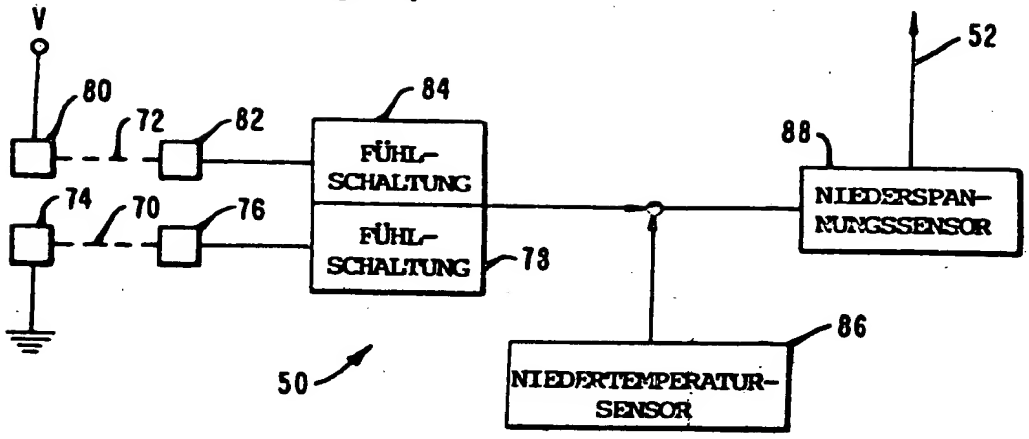


FIG. 8

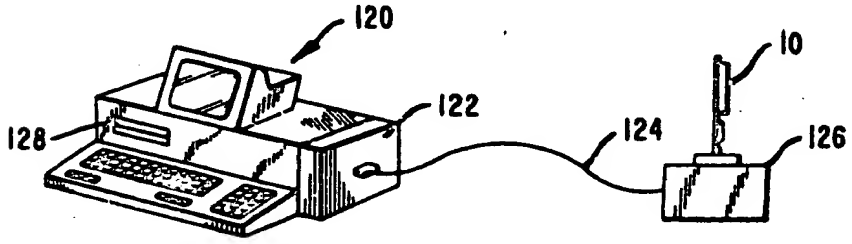


FIG. 5

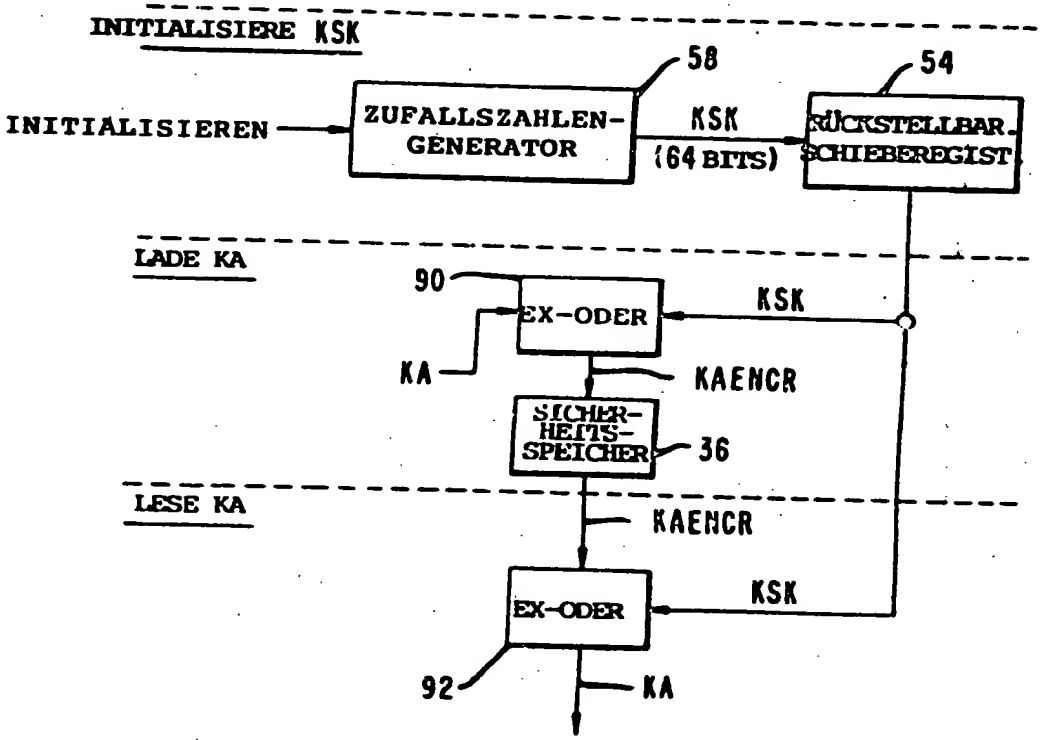

INITIALISIERE KSK
INITIALISIEREN
ZUFALLSZAHLEN-GENERATOR
58
KSK
(64 BITS)
54
RÜCKSTELLBAR. SCHIEBEREGIST
LADE KA
90
EX-ODER
KSK
KA
KAENCR
SICHER-HEITS-SPEICHER
36
LESE KA
KAENCR
EX-ODER
KSK
92
KA

FIG. 6

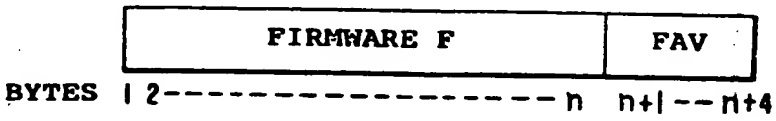

FIRMWARE F
FAV
BYTES 1 2---------- n n+1--n+4

FIG. 7

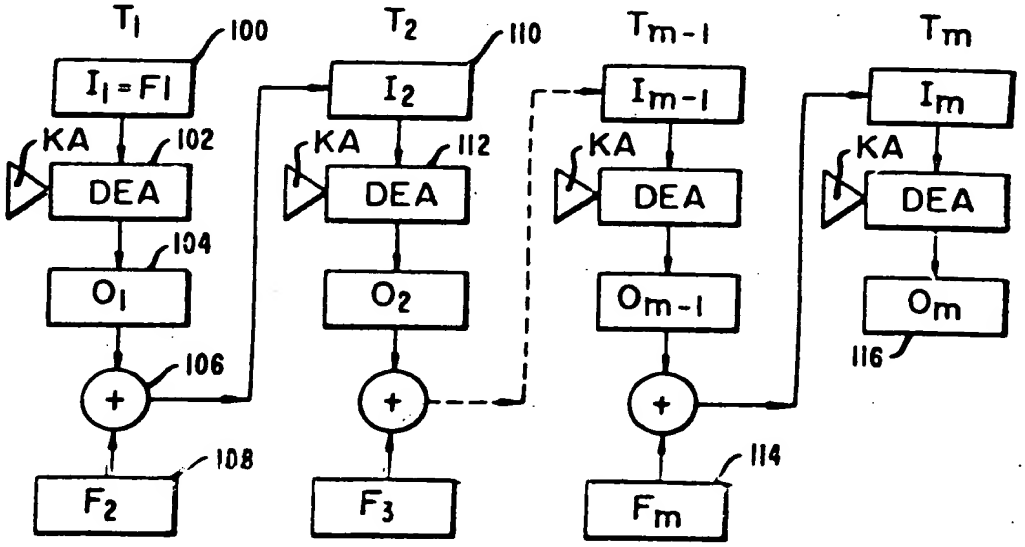
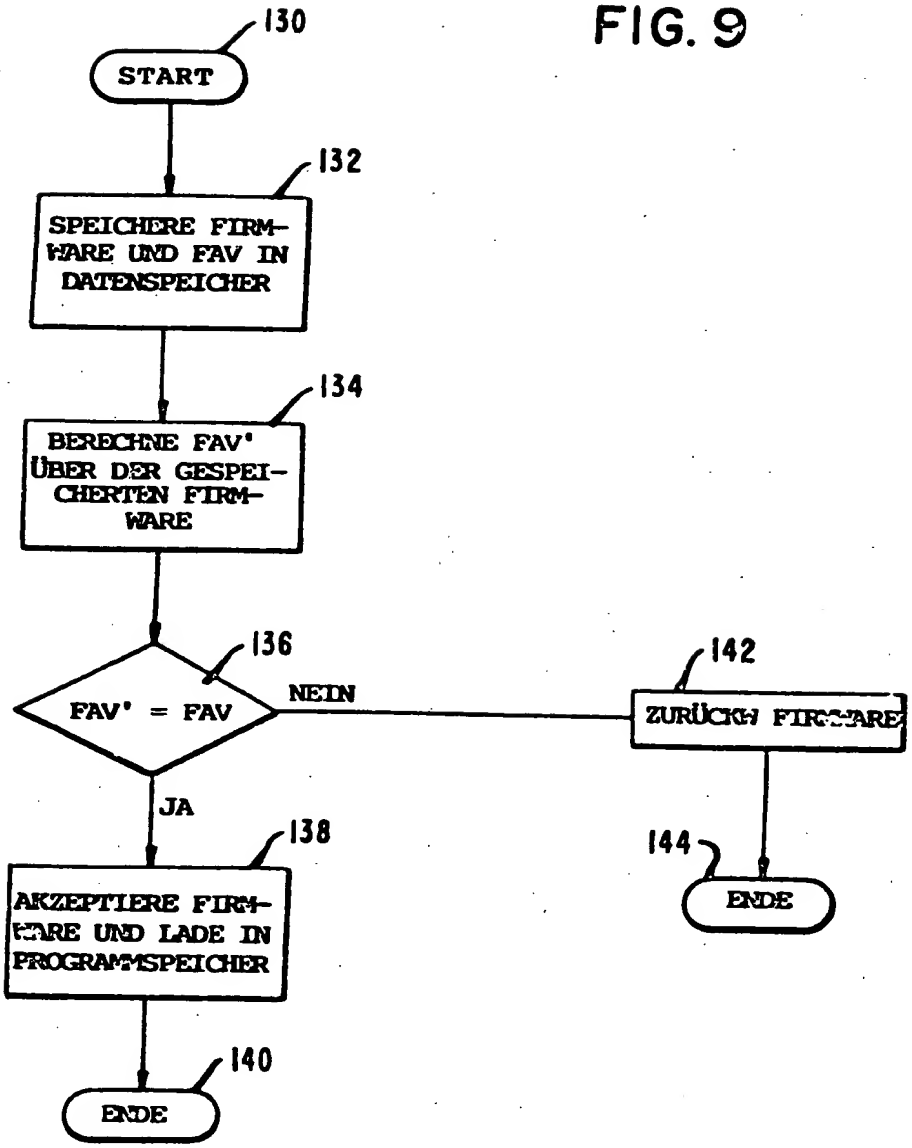

T1
100
I1 = F1
KA
102
DEA
104
O1
106
+
108
F2
T2
110
I2
KA
112
DEA
O2
+
F3
Tm-1
Im-1
KA
DEA
Om-1
+
114
Fm
Tm
Im
KA
DEA
Om
116

FIG. 9


130
START
132
SPEICHERE FIRMWARE UND FAV IN DATENSPEICHER
134
BERECHNE FAV' ÜBER DER GESPEICHERTEN FIRMWARE
136
FAV' = FAV
NEIN
142
ZURÜCK FIRMWARE
JA
138
AKZEPTIERE FIRMWARE UND LADE IN PROGRAMMSPEICHER
144
ENDE
140
ENDE